UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

ANDREW DUQUM, et al.,	)	
	)	
Plaintiffs,	)	
	)	Case No. 4:15-CV-1537-SPM
v.	)	
	)	
SCOTTRADE, INC.,	)	
	)	
Defendant.	)	

MEMORANDUM AND ORDER

This matter is before the Court on Defendant Scottrade, Inc.'s Motion to Dismiss Consolidated Class Action Complaint. (Doc. 58). The parties have consented to the jurisdiction of the undersigned United States Magistrate Judge pursuant to 28 U.S.C. § 636(c)(1). (Doc. 62). The motion has been fully briefed. For the following reasons, the motion will be granted.

I. FACTUAL BACKGROUND

Defendant is a firm that provides brokerage, banking, and retirement planning services to individuals and businesses. Consolidated Class Action Compl. ("Compl."), Doc. 40, ¶¶ 34-35. When a customer opens an account with Defendant, Defendant requires the customer to complete its Brokerage Agreement and provide personal information, including names, addresses, phone numbers, Social Security numbers, work history, and other personal identifying information (collectively, "PII"). *Id.* ¶ 37. The Brokerage Agreements incorporate the Scottrade Brokerage Privacy Statement, which states, "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings." *Id.* ¶¶ 37, 40. The Privacy Statement also indicates that Defendant collects personal information at other times and

collects personal information from others, such as credit bureaus. *Id.* ¶ 41. Defendant also has an Online Privacy Policy and other documents on its website indicating that it takes steps to protect the security of customer information. *Id.* ¶¶ 42-43.

Between September 2013 and February 2014, hackers gained access to Defendant's customer databases and exported confidential customer PII from those databases (the "data breach"). *Id.* ¶¶ 2, 59. The data breach was reported to involve the confidential information of approximately 4.6 million customers. *Id.* ¶ 48. The hackers took the PII for the purpose of building their own competing customer database for marketing and brokering stock transactions. *Id.* ¶ 62. They used the PII to operate a stock price manipulation scheme that amassed millions of dollars. *Id.* ¶ 74.

Defendant was unaware of the data breach until August 2015, when the FBI notified Defendant of it. *Id.* ¶¶ 75-76. On October 2, 2015, Defendant began notifying its customers about the data breach via email or mail. *Id.* ¶ 78. Defendant stated that it would provide one year of credit monitoring and identity theft insurance to affected persons, and it also suggested several actions customers could take themselves to detect or prevent fraud. *Id.* ¶¶ 84-88.

Shortly after Defendant announced the data breach, several of Defendant's customers filed putative class action lawsuits based on the data breach. On October 3, 2015, Plaintiff Stephen Hine filed his putative class action, *Hine v. Scottrade, Inc.*, No. 4:15-CV-01954-CEJ, in the United States District Court for the Southern District of California, and the case was subsequently transferred to this Court. On October 7, 2015, Plaintiff Andrew Duqum filed his putative class action, *Duqum v. Scottrade, Inc.*, No. 4:15-CV-01537-SPM, in this Court. On December 9, 2015, Plaintiff Matthew Kuhns filed his putative class action, *Kuhns v. Scottrade, Inc.*, No. 4:15-CV-01812-SPM, in this Court. On January 31, 2016, a fourth case, *Angela Martin*

v. Scottrade, Inc., No. 4:16-CV-00124-RWS, originally filed in the United States District Court for the Middle District of Florida, was also transferred to this Court. This Court subsequently consolidated all four cases pursuant to Fed. R. Civ. P. 42(a) and E.D. Mo. Local Rule 4.03. *See* Docs. 36 & 38.

On February 19, 2016, Plaintiffs filed their Consolidated Class Action Complaint, individually and on behalf of all others similarly situated.[1] Plaintiffs allege that they had accounts with Defendant and that as a result of the data breach, their PII was disclosed, transferred, sold, opened, read, mined, and otherwise used without their authorization. Compl. ¶¶ 9-12. Plaintiffs allege several causes of action against Defendant related to the data breach, including breach of contract, breach of implied contract, negligence, unjust enrichment/assumpsit, declaratory relief, and violations of various state consumer protection statutes.

II. DISCUSSION

In the instant motion, Defendant argues that Plaintiffs' Consolidated Class Action Complaint must be dismissed for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1), because Plaintiffs have not suffered an injury in fact and therefore do not have standing to bring suit in this Court under Article III of the United States Constitution. Defendant also argues that Plaintiffs' claims should be dismissed under Rule 12(b)(6) for failure to state a claim.

[1] Angela Martin is not named as a plaintiff in the Consolidated Class Action Complaint. However, another named Plaintiff, Richard Obringer, is included.

A. Defendant's Motion to Dismiss Under Rule 12(b)(1) for Lack of Subject Matter Jurisdiction

1. Legal Standard

A motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) may be either a "facial" challenge based on the face of the pleadings, or a "factual" challenge, in which the court considers matters outside the pleadings. *See Titus v. Sullivan*, 4 F.3d 590, 593 (8th Cir. 1993); *Osborn v. United States*, 918 F.2d 724, 729, n. 6 (8th Cir. 1990); *C.S. ex rel. Scott v. Mo. State Bd. of Educ.*, 656 F. Supp. 2d 1007, 1011 (E.D. Mo. 2009). Here, Defendant's challenge is based on the face of the pleadings and is therefore a facial attack. In evaluating a facial attack, "the court restricts itself to the face of the pleadings and the non-moving party receives the same protections as it would defending against a motion brought under Rule 12(b)(6)." *Branson Label, Inc. v. City of Branson, Mo.*, 793 F.3d 910, 914 (8th Cir. 2015) (quoting *Osborn*, 918 F.2d at 729 n. 6). The court must accept as true all of the factual allegations in the complaint, but it need not accept legal conclusions. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

2. Discussion

Under Article III, § 2 of the United States Constitution, federal jurisdiction is limited to "Cases" and "Controversies." U.S. Const. Art. III, § 2. "'One element of the case-or-controversy requirement' is that plaintiffs 'must establish that they have standing to sue.'" *Clapper v. Amnesty Int'l U.S.A.*, 133 S. Ct. 1138, 1146 (2013) (quoting *Raines v. Byrd*, 521 U.S. 811, 818 (1997)). The "irreducible constitutional minimum" of standing consists of three elements. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016) (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). "The plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Id.* "The plaintiff, as the party invoking federal jurisdiction, bears

the burden of establishing these elements." *Id.* (citing *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990)). Where a case is at the pleading stage, the plaintiff must "clearly . . . allege facts demonstrating each element." *Id.* (quoting *Warth v. Seldin*, 422 U.S. 490, 518 (1975)).

Only the injury in fact element of standing is at issue in this case. "To establish injury in fact, a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Id.* at 1548 (quoting *Lujan*, 504 U.S. at 560). "For an injury to be particularized, it must affect the plaintiff in a personal and individual way." *Id.* (quotation marks omitted). For an injury to be "concrete, it "must be '*de facto*'; that is, it must actually exist"; it must be real and not "abstract." *Id.*

In their Consolidated Class Action Complaint, Plaintiffs allege that they have suffered several categories of injury or harm related to the data breach: (a) increased risk of identity theft and identity fraud; (b) the financial and/or temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages; (c) failure to receive the full benefit of their bargain as a result of receiving brokerage and financial services that were less valuable than what they paid for; (d) deprivation in the value of their personal information; and (e) invasion of privacy and breach of the confidentiality of their personal information. *See* Compl. ¶ 15. Defendant contends that none of these alleged harms constitute an injury in fact that is "actual" or "imminent," arguing that the majority of courts faced with similar allegations have found these alleged harms too speculative or abstract to satisfy the injury in fact requirement. The Court will address each alleged type of alleged harm in turn.

i. Increased Risk of Identity Theft and Identity Fraud

Plaintiffs first allege that they face an "imminent, immediate and [] continuing increased risk of identity theft and identity fraud"[2] because their PII has been taken by hackers who have "disclosed [], transferred, sold, opened, read, mined, and otherwise used" Plaintiffs' PII without their authorization, to [the hackers'] financial benefit and to [Plaintiffs'] financial and other detriment." Compl. ¶¶ 9-12, 15. Plaintiffs allege that criminals can use PII for a variety of crimes, including credit card fraud, phone or utilities fraud, bank/finance fraud, obtaining a driver's license or official identification card in the victim's name, obtaining government benefits, filing a fraudulent tax return, obtaining a job using the victim's social security number, or receiving medical services in the victim's name. *Id.* ¶¶ 25-27. Defendant argues that Plaintiffs' allegations are insufficient to satisfy the injury in fact requirement, because they allege only the hypothetical possibility of harm.

As discussed above, to show an injury in fact, the plaintiff must show that he or she suffered an invasion of an interest that is "actual or imminent, not conjectural or hypothetical.'" *Clapper*, 135 S. Ct. at 1147 (quoting *Lujan*, 504 U.S. at 560). In *Clapper*, the Supreme Court addressed the circumstances under which a threatened future injury should be considered "imminent," such that the threatened injury satisfies the injury in fact requirement for Article III standing. The Supreme Court stated that it has "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact' and that 'allegations of *possible* future injury' are not sufficient." *Clapper*, 133 S. Ct. at 1147 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (emphasis in original). It expressly rejected the argument that it was sufficient to

[2] Plaintiffs allege that "identity theft" occurs when PII is used to commit fraud or other crimes, including credit card fraud, phone or utilities fraud, bank fraud, and government fraud. *See* Compl. ¶ 13 n.1

show an "objectively reasonable likelihood" of a threatened injury occurring. It also expressed a "reluctance to endorse standing theories that rest on speculation about decisions of independent actors" and noted that a theory of standing based on future injury that "relies on a highly attenuated chain of possibilities" about what independent actors might do does not satisfy the requirement that the threatened injury must be certainly impending. *Id.* at 1148-50.[3]

Both before and after the Supreme Court's decision in *Clapper*, most courts addressing standing in data breach cases have found that in the absence of some actual identity theft or other act harming the plaintiffs, the increased risk of future harm following a data breach does not constitute an injury in fact for purposes of Article III standing. *See In re SuperValu, Inc.*, No. 14-MD-2586 ADM/TNL, 2016 WL 81792, at *4-*5 (D. Minn. Jan. 7, 2016) (noting that "[i]n data security breach cases where plaintiffs' data has not been misused following the breach, the vast majority of courts have held that the risk of future identity theft or fraud is too speculative to constitute an injury in fact for purposes of Article III standing"; finding no injury in fact based on increased risk of future harm where the plaintiffs' PII was stolen in a large data breach but the only incident of actual misuse of information alleged was a single unauthorized credit card charge not clearly traceable to the breach); *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 955-58 (D. Nev. 2015) (noting that "[t]he majority of courts dealing with data-breach cases post-*Clapper* have held that absent allegations of actual identity theft or other fraud, the increased risk of such harm alone is insufficient to satisfy Article III standing"; finding no injury in fact based on increased risk of future harm where the plaintiffs' PII was stolen in a large data breach but no plaintiff had alleged that any unauthorized purchases or other manifestations of misuse of their

[3] In a footnote, the Supreme Court in *Clapper* also noted that it has "in some instances . . . found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm," though it did not explain the circumstances under which that standard would apply. *Id.* at 1147 n. 5.

PII had occurred); *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 28 (D.D.C. 2014) (noting that "since *Clapper* was handed down last year, courts have been even more emphatic in rejecting 'increased risk' as a theory of standing in data-breach cases" and that "[m]ost cases that found standing . . . were decided pre-*Clapper* or rely on pre-*Clapper* precedent and are, at best, thinly reasoned").[4]

These courts often emphasize that the asserted risk of harm is too speculative and hypothetical to satisfy the imminence requirement because it depends on speculation about the actions of independent actors—the hackers or other criminals. Whether the plaintiffs will actually suffer the threatened harm depends on whether the hackers actually obtained the PII, whether they intend to use the PII to commit acts that would be detrimental to the plaintiffs, whether they are capable of using the PII to commit acts detrimental to the plaintiffs, and whether they actually do use the information to commit acts detrimental to the plaintiffs, such as making unauthorized transactions in the plaintiffs' names. *See, e.g., In re SuperValu, Inc.*, 2016 WL 81792, at *5 (increased risk of harm was too speculative to constitute an injury in fact, in part because the court was required "to speculate about whether the hackers who gained access

[4] *See also, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42-45 (3d Cir. 2011) (no injury in fact based on increased risk of harm where there were no allegations that the data exposed in the breach had actually been misused to the plaintiffs' detriment); *Whalen v. Michael Stores, Inc.*, --- F. Supp. 3d ----, No. 14-CV-7006(JS)(ARL), 2015 WL 9462108, at *4-*5 (E.D.N.Y. Dec. 28, 2015) (no injury in fact based on an increased risk of harm where hackers stole credit and debit card information from retailer's systems); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 365-66 (M.D. Pa. 2015) (no injury in fact based on increased risk of harm where the plaintiffs alleged that hackers obtained and misappropriated their personal data but did not allege that the hackers actually committed any identity theft or other crime); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 654-57 (S.D. Ohio 2014) (no injury in fact based on increased risk of harm where plaintiffs alleged that their PII was stolen and disseminated but did not allege that they had been victimized by identity theft, identity fraud, medical fraud, or phishing); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052-53 (E.D. Mo. 2009) (no injury in fact based on increased risk of harm where it was unclear whether plaintiff's information had been compromised in the breach and when, if ever, it would be fraudulently used to cause him harm).

to [the breached network] were able to capture or steal Plaintiffs' PII; whether the hackers or other criminals will attempt to use the PII; and whether those attempts will be successful"); *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 959 (increased risk of harm was too speculative to constitute an injury in fact where the possibility of harm depended "entirely on the decisions or capabilities of an independent, and unidentified, actor"); *Fernandez v. Leidos, Inc.*, 127 F. Supp. 3d 1078, 1087 (E.D. Cal. 2015) ("Plaintiff's allegations concerning his increased risk of harm require speculation about the decisions or capabilities of independent, unidentified actors,—the data thief or thieves, and whether they intend to misuse [the data] at some point in the future") (quotation marks and alterations omitted); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1052-53 (E.D. Mo. 2009) (no injury in fact in a data breach case where the plaintiff would only be injured if many "ifs" came to pass—"'if' his personal information was compromised, and 'if' such information was obtained by an unauthorized third party, and 'if' his identity was stolen as a result, and 'if' the use of his stolen identity caused him harm"); *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 655 (S. D. Ohio 2014) ("[W[hether Named Plaintiffs will become victims of theft or fraud . . . is entirely contingent on what, if anything, the third party criminals do with that information.").

These courts also often consider whether a significant period of time has passed since the breach without the plaintiffs having suffered the threatened injury, because "[a]s more time lapses without the threatened injury actually occurring, the notion that the harm is imminent becomes less likely." *In re SuperValu, Inc.*, 2016 WL 81792, at *5 (no injury in fact where "the passage of nearly a year and a half without the occurrence of harm traceable to the Data Breach makes it unlikely that such threatened harm is imminent"). *See also Storm v. Paytime*, 90 F. Supp. 3d 359, 366-67 (M.D. Pa. 2015) (no injury in fact where the passage of almost a year with

no plaintiffs becoming actual victims of identity theft undermined the notion that the identity theft was imminent); *In re Zappos.com*, 108 F. Supp. 3d at 958-59 (no injury in fact where three and a half years had passed without a single allegation of theft or fraud).

Here, although Plaintiffs have alleged that the hackers accessed Plaintiffs' PII and used that PII for certain illegal business enterprises, Plaintiffs do not allege any of the PII stolen in the breach has been used to commit any identity theft, fraud, or any other act that has resulted in harm to any plaintiff. Nor do Plaintiffs allege any facts that suggest that the hackers intend to commit identity theft, fraud, or any other act that would result in harm to any plaintiff. Thus, as in the above cases, the Court cannot determine whether Plaintiffs will suffer harm in the future without engaging in considerable speculation about the hackers' possible intentions and future actions. Plaintiffs will suffer harm only *if* the hackers actually intend to use Plaintiffs' PII to commit identity theft, fraud, or some other act that might harm Plaintiffs; *if* the hackers attempt to use the PII to commit such identity theft, fraud, or other act; *if* they actually succeed in doing so; and *if* the identity theft, fraud, or other act causes harm to Plaintiffs. In light of the uncertainty over whether any of these events will occur, the Court cannot find that Plaintiffs face any harm that is "certainly impending." This conclusion is strengthened by the fact that more than two years have passed since the original data breach without a single alleged instance of identity theft or fraud involving any of Defendant's customers. [5]

[5] Even assuming that the "substantial risk" standard mentioned in the *Clapper* footnote could somehow apply here instead of the "certainly impending" standard, the Court also finds that standard is not satisfied for the same reasons that the "certainly impending" standard is not satisfied. *See, e.g.*, *In re Supervalu, Inc.*, 2016 WL 81792, at *5 (plaintiffs failed to show that there was a substantial risk that harm would occur from a data breach where there had been no incidents harming plaintiffs in over a year and where the occurrence of the harm depended on speculation about what the hackers would do); *Fernandez*, 127 F. Supp. 3d at 1087 (no "substantial risk" of harm from data breach where allegations concerning risk of harm required speculation about the future actions of a third party).

Plaintiffs emphasize that here, unlike in some of the cases relied on by Defendant in which it was unclear whether the plaintiffs' information had been accessed or whether the hackers had malicious intent, the hackers here actually accessed the PII and used it for unlawful purposes. However, those allegations do not change the Court's conclusion. First, some of the cases relied on by Defendant did involve allegations that data had actually been accessed by hackers with malicious intent. *See In re Zappos, Inc.*, 108 F. Supp. 3d at 958 (increased risk of harm was too speculative to support standing even where PII was "stolen" and even "[i]f the Court assumes that the hacker or some other nefarious third-party remains in possession of Plaintiffs' personal information"); *Storm*, 90 F. Supp. 3d at 366 (no injury in fact despite allegations that the plaintiffs' PII had been "stolen," "accessed," and "misappropriated"). Second, although the Court does not need to speculate about whether the hackers here will actually access the PII or whether they have malicious intent, the Court is still required to speculate about whether they intend to commit any acts (such as identity theft) that might actually harm any of the individual plaintiffs, whether they will succeed in committing those acts, and whether those acts will result in actual harm to Plaintiffs. As discussed above, in light of that uncertainty about the intentions and possible actions of third parties, the Court cannot find that any harm to Plaintiffs is "certainly impending" or that there is a substantial risk of it occurring, particularly in light of the passage of more than two years without it having occurred.

Plaintiffs also argue that instead of relying on the cases discussed above, the Court should rely on *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). In that case, 350,000 credit card numbers were exposed to a data breach by hackers, and within a few months of the breach, fraudulent charges had been made on 9,200 of the cards. *Id.* at 690. The court found that the holders of the other cards had standing to sue based on the imminent risk of future

harm to them, noting that they "should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur." *Id.* at 693. As a preliminary matter, the Court notes that it appears that the Seventh Circuit was using the "objectively reasonable likelihood" standard that was rejected by the Supreme Court in *Clapper*. *See Clapper*, 133 S. Ct. at 1147 ("[T]he Second Circuit's 'objectively reasonable likelihood' standard is inconsistent with our requirement that 'threatened injury must be certainly impending to constitute injury in fact.'"). Moreover, to the extent that the Seventh Circuit was applying the appropriate standard, it is factually distinguishable. The 9,200 fraudulent charges in *Remijas* demonstrated that the hackers in that case intended to use, were capable of using, and were actually using the stolen data to create fraudulent credit card charges as to some cardholders, which significantly increased the likelihood that they intended to do the same with regard to the remaining cardholders and would be capable of doing so. That fact distinguishes *Remijas* from the instant case, in which more than two years have passed with no incidents of identity theft or other actual harm to the individuals whose PII was taken.

The other cases relied on by Plaintiffs are similarly distinguishable *See Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 965 (7th Cir. 2016) (several fraudulent transactions were made on one of the plaintiff's cards shortly after the data breach); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010) (after a laptop containing unencrypted personal data was stolen, one of the plaintiffs alleged that someone attempted to open a bank account in his name);[6] *In re Adobe Sys., Inc. Privacy Litig.*, 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014) (data stolen by hackers had surfaced on the internet). Moreover, to the extent that these cases cannot

[6] Significantly, *Krottner* predated *Clapper* and does not address or discuss either the "certainly impending" standard or the "substantial risk" standard.

be distinguished from the instant case, the Court finds them less persuasive than the cases cited by Defendant, because they are less consistent with *Clapper*'s holding that a threatened injury must be "certainly impending" to satisfy the injury-in-fact requirement, as well as its suggestion that courts should be "reluctan[t] to endorse standing theories that rest on speculation about decisions of independent actors." *See Clapper*, 133 C. Ct. at 1147-50.

For all of the above reasons, the Court finds that Plaintiffs' allegations regarding the increased risk of identity theft and fraud are not sufficient to demonstrate injury in fact for purposes of Article III standing.

ii. Costs of Monitoring and Mitigation

Plaintiffs also allege that they have suffered injury in the form of the alleged financial and/or temporal costs of monitoring their credit, monitoring their financial accounts, and mitigating their damages. Compl. ¶ 15. Defendant argues that because the risk of future harm that forms the basis for the alleged need for monitoring or mitigation is not imminent, the cost to monitor for it or mitigate the risk of it is not sufficient to confer Article III standing.

In *Clapper*, the Supreme Court found that plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." 133 S. Ct. 1151. "If the law were otherwise, an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear." *Id.* Consistent with *Clapper*, "[i]n data breach cases, courts consistently hold that the cost to mitigate the risk of future harm does not constitute an injury in fact unless the future harm being mitigated against is itself imminent." *In re SuperValu, Inc.*, 2016 WL 81792, at *7 (citing cases). *See also Reilly v. Ceridian Corp.*, 664 F.3d 38, at 46 (3d Cir. 2011) ("[A]lleged time and money expenditures to monitor [plaintiffs'] financial

information do not establish standing, because costs incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for [plaintiffs'] claims."); *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 961 ("The Court's finding here that the threat of future theft or fraud is not sufficiently imminent to confer standing compels the conclusion that incurring costs to mitigate that threat cannot serve as the basis for this action.").

Here, because the Court has already found that Plaintiffs' increased risk of identity theft or fraud is does not constitute an imminent harm, the cost of monitoring for that risk or mitigating that risk cannot constitute an injury in fact.

iii. Failure to Receive the Full Value of Bargained-for Services

Plaintiffs next allege that they have been injured as a result of the data breach because they received brokerage and financial services that were less valuable than the ones they paid for. Compl. ¶ 14. Specifically, they allege that Plaintiffs bargained for, and expected to receive, data security measures safeguarding and protecting the privacy of their PII, Compl. ¶ 45; that a portion of the brokerage and financial services fees Plaintiffs paid was for data management and data security, Compl. ¶ 14; and that Plaintiffs would not have opened accounts with Defendant, or would not have paid as much with respect to those accounts, had they known that Defendant failed to take reasonable precautions to secure PII, Compl. ¶ 46.

A majority of courts have found that similar allegations of loss of bargained-for services in data breach cases are not sufficiently concrete to satisfy the injury in fact requirement of Article III standing. *In re SAIC*, 45 F. Supp. 3d at 30 ("To the extent that Plaintiffs claim that some indeterminate part of their premiums went toward paying for security measures, such a claim is too flimsy to support standing. They do not maintain, moreover, that the money they

paid could have or would have bought a better policy with a more bullet-proof information-security regime. Put another way, Plaintiffs have not alleged facts that show that the market value of their insurance coverage (plus security services) was somehow less than what they paid."); *Fernandez*, 127 F. Supp. 3d at 1089 (no injury in fact based on lost benefit of the bargain because "Plaintiff has not alleged facts from which a plausible inference could be drawn that he has been injured by a loss in value of his insurance coverage, nor has he alleged that the value of his health care coverage after the Data Breach is less than what it was before the Data Breach."); *In re SuperValu, Inc.*, 2016 81792, at *8 (rejecting the plaintiffs' argument that they were harmed by the lost benefit of their bargain; noting that the plaintiffs did "not allege that the Data Breach diminished the value of the groceries or other goods they purchased from Defendants" and did not "allege facts showing that the price they paid for the goods included an amount that both parties understood would be allocated toward protecting customer data."); *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 962 n.5 (rejecting theory that plaintiffs had standing based on an alleged decrease in the value of Zappos's services, where the plaintiffs did "not explain how the data breach impacted the value of the goods they purchased from Zappos" and did not "allege facts showing how the price they paid for such goods incorporated some particular sum that was understood by both parties to be allocated towards the protection of customer data"). *See also Remijas*, 794 F.3d at 694-95 (noting in *dicta* that the benefit of the bargain theory was "problematic" and "dubious" where plaintiffs had not alleged any defect in any product they purchased). *But see In re Anthem Data Breach Litig.*, No. 15-md-02617, 2016 WL 589760, at *27 (N.D. Cal. Feb. 14, 2016) (loss of benefit of the bargain sufficient to show injury in fact where the plaintiffs alleged that had the defendants disclosed that their computer systems and data security practices were inadequate, the plaintiffs would not have enrolled in the defendants'

health care plans); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 860-61 (N.D. Cal. 2011)) (finding plaintiff had alleged injury in fact based on lost benefit of the bargain theory; noting that plaintiff was setting forth a "novel theory" and that there was a "paucity of controlling authority" on the issue).

Here, Plaintiffs do not allege facts from which a plausible inference could be drawn that Plaintiffs received services from Defendant that were less valuable than those Plaintiffs bargained for. Although they allege in a conclusory fashion that a portion of the brokerage fees they paid to Defendant were for "data management and security," they do not allege any facts showing how any fee they paid was understood by both parties to be allocated toward the protection of customer data. Nor do Plaintiffs allege that the money they paid could have or would have bought a better policy with a more bullet-proof data-security regime. Thus, Plaintiffs have not alleged an injury sufficiently concrete to satisfy Article III's injury in fact requirement.

iv. Deprivation in Value of Plaintiffs' Personal Information

Plaintiffs also allege that as a result of the data breach, they have suffered (and will continue to suffer) economic damages and other injury and harm in the form of the deprivation of the value of their PII, for which there is a well-established national and international market. Compl. ¶ 13. Plaintiffs allege that they have a valuable property right in their PII and that Plaintiffs, not data thieves, should have the exclusive right to monetize their PII. *Id.* They allege that "[f]aced with the choice of having their PII . . . used without their authorization versus selling their PII on the black market and receiving the compensation themselves, Plaintiffs would choose the latter." *Id.*

Most courts have found that similar allegations are insufficient to demonstrate an injury in fact. *See, e.g.*, *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 954 (finding no injury in fact based

on deprivation of value of personal information; noting that "Even assuming that Plaintiffs' data has value on the black market, Plaintiffs do not allege any facts explaining how their personal information became less valuable as a result of the breach or that they attempted to sell their information and were rebuffed because of a lower price-point attributable to the security breach"); *Fernandez.*, 127 F. Supp. 3d at 1087 (finding no injury in fact based on deprivation of value of PII where plaintiff "has not alleged that he intended to sell his [PII], that he plans to sell it in the future, that he is foreclosed from doing so because of the Data Breach, or that the data breach reduces the value of the [PII] he possesses"); *Galaria*, 998 F. Supp. 2d at 660 (no injury in fact based on deprivation of value of personal information where plaintiffs failed to allege that the breach actually prevented them from selling their information at the price they claimed it was worth); *In re SuperValu, Inc.*, 2016 WL 81792, at *7 (no injury in fact based on deprivation of value of personal information where "Plaintiffs have failed to allege any facts explaining how their PII became less valuable as a result of the Data Breach.").

Here, as in the above cases, Plaintiffs do not allege any facts showing how their PII became less valuable as a result of the data breach. Although Plaintiffs allege that they would rather sell their PII on the black market than have it used without their authorization, they do not allege that they ever intended to sell their information on the black market, that they ever attempted to sell it after the data breach and were unable to do so, or that they ever attempted to sell it after the data breach and were forced to accept a lower price than they would have had the data breach not occurred. Nor do they allege any other facts suggesting that they have been foreclosed from capitalizing on the value of their personal information because of the data breach. Therefore, as in the above cases, Plaintiffs have not alleged an injury sufficiently concrete to satisfy Article III's injury in fact requirement.

v. Invasion of Privacy and Breach of Confidentiality

Plaintiffs next assert that they have suffered an invasion of privacy and a breach of confidentiality, alleging that consumers place a high value on the privacy of their personal data.

Courts have held that loss of privacy and breach of confidentiality are too abstract to establish Article III standing. *See In re SuperValu, Inc.*, 2016 WL 81792, at *8 (allegations of loss of privacy and confidentiality did not support standing because plaintiffs "have not alleged facts showing that the loss of privacy and confidentiality resulted in a concrete injury"); *In re Zappos.com*, 108 F. Supp. 3d at 962 n.5 ("Even if Plaintiffs adequately allege a loss of privacy, they have failed to show how that loss amounts to a concrete and particularized injury"; noting that "Plaintiffs do not claim that they have suffered any damages due to a loss of privacy").

Here, Plaintiffs do not allege any facts demonstrating that they suffered any damages or injury due to a loss of privacy or breach of confidentiality. These theories are not sufficiently concrete to establish injury in fact and do not support standing in this case.

For all of the above reasons, Plaintiffs have failed to plead facts demonstrating that they have suffered any injury in fact. Therefore, Plaintiffs lack standing, and this case must be dismissed for lack of subject matter jurisdiction. Because the dismissal is for lack of standing under Rule 12(b)(1), the dismissal is without prejudice. *See In re SuperValu, Inc.*, 2016 WL 81792, at *8; *In re Zappos.com, Inc.*, 108 F. Supp. 3d at 962.

B. Motion to Dismiss Under Rule 12(b)(6) for Failure to State a Claim

Because the Court concludes that it is without subject matter jurisdiction over this case, the Court need not address Defendant's motion to dismiss for failure to state a claim under Rule 12(b)(6).

III. CONCLUSION

For all of the above reasons,

IT IS HEREBY ORDERED that Defendant Scottrade, Inc.'s Motion to Dismiss Consolidated Class Action Complaint. (Doc. 58) is **GRANTED**.

IT IS FURTHER ORDERED that Defendant Scottrade, Inc.'s earlier Motion to Dismiss (Doc. 19), which was addressed to the Complaint that was filed by Andrew Duqum prior to the filing of the Consolidated Class Action Complaint, is **DENIED** as moot.

IT IS FURTHER ORDERED that Plaintiffs' Consolidated Class Action Complaint (Doc. 40) is **DISMISSED** without prejudice.

SHIRLEY PADMORE MENSAH
UNITED STATES MAGISTRATE JUDGE

Dated this 12th day of July, 2016.